DOCKET No.
NAI1P093/02.012.01

U.S. PATENT APPLICATION

FOR A

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A FIREWALL SUMMARY INTERFACE

20020059457.pdf

ASSIGNEE: McAfee.com Corporation

SILICON VALLEY IP GROUP
P.O. BOX 721120
SAN JOSE, CA 95172

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A FIREWALL SUMMARY INTERFACE

FIELD OF THE INVENTION

The present invention relates to firewalls, and more particularly to graphical user interfaces associated with firewalls.

BACKGROUND OF THE INVENTION

In the space of just a few years, the Internet--because it provides access to information, and the ability to publish information, in revolutionary ways--has emerged from relative obscurity to international prominence. Whereas in general an internet is a network of networks, the Internet is a global collection of interconnected local, mid-level, and wide-area networks that use the Internet Protocol (IP) as the network layer protocol. Whereas the Internet embraces many local- and wide-area networks, a given local- or wide-area network may or may not form part of the Internet.

As the Internet and its underlying technologies have become increasingly familiar, attention has become focused on Internet security and computer network security in general. With unprecedented access to information has also come unprecedented opportunities to gain unauthorized access to data, change data, destroy data, make unauthorized use of computer resources, interfere with the intended use of computer resources, etc. As experience has shown, the frontier of cyberspace has its share of scofflaws, resulting in increased efforts to protect the data, resources, and reputations of those embracing intranets and the Internet.

Firewalls are intended to shield data and resources from the potential ravages of computer network intruders. In essence, a firewall functions as a mechanism which monitors and controls the flow of data between two networks, or a network and a device. All communications, e.g., data packets, which flow between the networks in either direction must pass through the firewall; otherwise, security is circumvented. The firewall selectively permits the communications to pass from one network to another network or device, to provide bidirectional security.

Recently, there has been much work on software applications referred to as "personal firewalls." These applications are typically installed on a computer or any other computing device for protecting against unsecure networks coupled thereto. During use of such personal firewalls, network traffic is monitored and filtered based on a predetermined set of rules. Such rules may include any filtering criteria that are configured to protect the device from intrusion activity. For example, such criteria may result in: the prevention of computers having certain IP addresses from accessing the protected device, precluding access to certain ports associated with the protected device, the prevention of certain applications from accessing the protected device, etc. During use, a vast number of events may occur where network traffic is prevented based on the filtering criteria.

Often, a user may desire to modify the filtering criteria to tailor security for a particular device. Further, the user may wish to monitor the events to assess the current state of security of the device for the purposes of modifying the filtering criteria in the foregoing manner. With the state of security being extremely dynamic, there is a need to assess security and configure the personal firewall in a manner that is quick and effective. Unfortunately, prior art graphical user interfaces that allow a user to carry out such tasks are not integrated, and are cumbersome to use. For example, prior art personal firewalls merely list events, requiring the user to manually filter and analyze the data for the purpose of making a conclusion as to the current state of security of the device.

10019569.020202

There is thus a need for an interface system and method capable of facilitating the assessment of a current state of security of a device and the configuration process associated with a personal firewall used to protect such device.

5

10074586.020802

DISCLOSURE OF THE INVENTION

A system, method and computer program product are provided for summarizing firewall activity. Initially, a plurality of types of events associated with a firewall of a local computer is organized. Further, a number of occurrences of each type of event is tracked utilizing the firewall. Further, a graphical representation is displayed indicating a severity of the number of the events utilizing the firewall.

In one embodiment, the events may include blocked attempts of various types. One of the types of the blocked attempts may include blocked attempts of remote computers to access predetermined banned ports associated with the local computer. Further, one of the types of the blocked attempts may include blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer. Still yet, one of the types of the blocked attempts may include blocked attempts to access a network made by predetermined applications. As an option, the various types of the blocked attempts may be organized into categories.

In another embodiment, additional information may be displayed. For example, a plurality of banned ports associated with the first type of the blocked attempts may be displayed with the number of the occurrences associated therewith. Further, a plurality of banned IP addresses associated with the second type of the blocked attempts may be displayed with the number of the occurrences associated therewith. Still yet, a plurality of banned applications associated with the third type of the blocked attempts may be displayed with the number of the occurrences associated therewith.

In still another embodiment, the number of occurrences of each type of event that occur within a predetermined time period may be displayed. Moreover,

additional information relating to the events may be displayed upon the selection of the event, in a drill down manner.

For management purposes, a menu may also be displayed for selecting from a summary page, an applications page, an event log, and an IP address page. Upon the selection of the applications page on the menu, an applications interface may be displayed for selecting the predetermined applications. Upon the selection of an IP address page on the menu, an IP address interface may be displayed for selecting the predetermined IP addresses associated with the remote computers to be blocked. Still yet, upon the selection of an event log on the menu, a log of the events may be displayed.

For providing a quick reference as to the severity of the tally of each of the events, the graphical representation may include a bar graph. For example, a number of dots or other type of character may be used which is proportional to the severity of the total number of events. Optionally, a graphical representation may be displayed for each type of event.

A system, method and computer program product are provided for managing a firewall and reporting firewall activity associated therewith. Displayed in a first portion of an event log is a plurality of events. Upon the selection of one of the events, displayed in a second portion of the event log is information relating to the event. Further displayed is a menu in a third portion of the event log for selecting from a summary page for summarizing the events, an application selection page for selection of applications to be subject to security restrictions, and an Internet Protocol (IP) address selection page for selection of IP addresses to be subject to security restrictions.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure **1** illustrates an exemplary network environment, in accordance with one embodiment.

Figure **2** shows a representative hardware environment associated with the computers of Figure **1**.

Figure **3** is a flowchart of a method for summarizing firewall activity, in accordance with one embodiment.

Figure **4** illustrates an exemplary summary page, in accordance with operation **310** of Figure **3**.

Figure **5** illustrates an exemplary event log illustrating various traffic events that may be monitored by the firewall, in accordance with operation **318** of Figure **3**.

Figures **6A-6E** illustrate a plurality of options available to the user of the firewall, in accordance with various embodiments.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure **1** illustrates a network architecture **100**, in accordance with one embodiment. As shown, a plurality of networks **102** is provided. In the context of the present network architecture **100**, the networks **102** may each take any form including, but not limited to a local area network (LAN), a wide area network (WAN) such as the Internet, etc.

Coupled to the networks **102** are data computers **104** which are capable of communicating over the networks **102**. Also coupled to the networks **102** and the data computers **104** is a plurality of end user computers **106**. In the context of the present description, such computers may include a web server, desktop computer, lap-top computer, hand-held computer, printer or any other type of hardware/software network device. More detail regarding an exemplary embodiment of such data computers **104** and user computers **106** will be set forth hereinafter during reference to Figure **2**. A gateway **108** may optionally be coupled between the various computers.

One or more of the data computers **104** or user computers **106** may be equipped with a firewall. In one example, the firewalls may each include a software application installed directly on the data computers **104** or user computers **106** in the form of personal firewalls. Of course, other traditional approaches may also be employed. For example, a separate hardware component may be coupled between the computers and a network.

The firewalls installed on the data computers **104** or user computers **106** may be equipped with the ability of summarizing firewall activity. Initially, a plurality of types of events associated with the firewall of the computer is organized. Further, a number of occurrences of each type of event is tracked utilizing the firewall.

Further, a graphical representation is displayed indicating a severity of the number of the events utilizing the firewall.

For managing the firewall and reporting firewall activity associated therewith, an enhanced firewall graphical user interface may also be provided. Displayed in a first portion of an event log is a plurality of events. Upon the selection of one of the events, displayed in a second portion of the event log is information relating to the event. Further displayed is a menu in a third portion of the event log for selecting from a summary page for summarizing the events, an application selection page for selection of applications to be subject to security restrictions, and an Internet Protocol (IP) address selection page for selection of IP addresses to be subject to security restrictions.

By this design, an enhanced firewall summary and control interface are provided for allowing a user to better gauge the status of filtering carried out by the firewall. Further, the interface disclosed allows the user to more effectively configure the firewall in response to the status provided by the firewall summary. More information regarding exemplary interfaces employing these features will be set forth hereinafter in greater detail.

Figure **2** shows a representative hardware environment that may be associated with the data computers **104** and/or end user computers **106** of Figure **1**, in accordance with one embodiment. Such figure illustrates a typical hardware configuration of a workstation in accordance with a preferred embodiment having a central processing unit **210**, such as a microprocessor, and a number of other units interconnected via a system bus **212**.

The workstation shown in Figure **2** includes a Random Access Memory (RAM) **214**, Read Only Memory (ROM) **216**, an I/O adapter **218** for connecting peripheral devices such as disk storage units **220** to the bus **212**, a user interface adapter **222** for connecting a keyboard **224**, a mouse **226**, a speaker **228**, a

microphone **232**, and/or other user interface devices such as a touch screen (not shown) to the bus **212**, communication adapter **234** for connecting the workstation to a communication network **235** (e.g., a data processing network) and a display adapter **236** for connecting the bus **212** to a display device **238**.

The workstation may have resident thereon an operating system such as the Microsoft Windows NT or Windows/95 Operating System (OS), the IBM OS/2 operating system, the MAC OS, or UNIX operating system. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. A preferred embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, along with an object oriented programming methodology. Object oriented programming (OOP) has become increasingly used to develop complex applications.

Figure **3** is a flowchart of a method **300** for summarizing firewall activity, in accordance with one embodiment. As an option, the present method **300** may be carried out in the network architecture **100** of Figure **1**. Of course, however, the present method **300** may be executed in any desired context and environment.

Initially, in operation **301**, a firewall is executed in association with a local computer. As mentioned earlier, the firewall may include a software application installed directly on the computer in the form of a personal firewall. Of course, other traditional approaches may also be employed including the use of a separate hardware component coupled between the computer and a network.

Initially, in operation **302**, a plurality of events is tracked utilizing the firewall. Next, a number of such events is tracked in operation **304**. In the context of the present description, such traffic events may include successful and/or blocked attempts to access (i.e. communicate with) the local computer, and/or attempts of the local computer to access (i.e. communicate with) a network.

In one embodiment, the blocked attempts may be of various types. One of the types of the blocked attempts may include blocked attempts of remote computers to access predetermined banned ports associated with the local computer. Further, one of the types of the blocked attempts may include blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer. Still yet, one of the types of the blocked attempts may include blocked attempts to access a network made by predetermined applications. As an option, the various types of the blocked attempts may be organized into categories.

In operation **306**, a menu is displayed for selecting from a plurality of interface features including a summary page, an applications page, an event log, a trusted IP address page, and a banned IP address page. Such selection is determined by decision **310**. As will soon become apparent, such options provide an enhanced firewall summary and control interface for allowing a user to better gauge the status of filtering carried out by the firewall. Further, such interface allows the user to more effectively configure the firewall in response to the status provided by the firewall summary.

Upon the selection of the summary page on the menu, a summary page is displayed including a recent activity list, frequently accessed port list, commonly blocked IP address list, and commonly blocked application list. See operation **310**. It should be noted that the summary page may be displayed in response to an active selection made using the menu and/or automatically displayed with the menu at start-up. Further displayed as a component of the summary page is a graphical representation indicating a severity of a number of the events detected utilizing the firewall.

For providing a quick reference as to the severity of the tally of each of the events, the graphical representation may include a bar graph. For example, a number of dots or other type of character may be used which is proportional to the severity of the total number of events. Such proportionality may be determined in any desired

10071586.020802

manner (i.e. using predefined equations, look-up table, etc.). As an option, the graphical representation may be displayed for each type of event. Further information regarding an exemplary summary page and related graphical severity representation will be set forth hereinafter in greater detail during reference to Figure 4.

Upon the selection of the applications page on the menu, an applications interface is displayed for selecting the predetermined applications. See operation **312**. This selection may be used to configure the firewall filtering in a user-defined manner. As mentioned earlier, one of the types of the attempts blocked by the firewall may include blocked attempts to access a network made by predetermined applications. Such applications may include, but are not limited to network browser applications, e-mail applications, file transfer protocol (FTP) applications, etc.

Upon the selection of the trusted IP address page on the menu, a trusted IP address interface is displayed for allowing a user to select the predetermined trusted IP addresses associated with remote computers not to be blocked. See operation **314**. In a similar manner, an untrusted IP address interface is displayed for selecting the predetermined untrusted IP addresses associated with remote computers to be blocked, upon the selection of the untrusted IP address page on the menu. Note operation **316**. As mentioned earlier, one of the types of the blocked attempts may include blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer.

Upon the selection of the event log on the menu, a log of events is displayed in accordance with operation **318**. More information relating to an exemplary event log will be set forth during reference to Figure **5**.

Figure **4** illustrates an exemplary summary page **400**, in accordance with operation **310** of Figure **3**. It should be noted that the present interface is presented

for illustrative purposes only, and any desired summary may be displayed to carry out the foregoing functionality.

As mentioned earlier, a menu **402** may also be displayed for selecting from a summary page icon **404** for displaying a summary in accordance with operation **310** of Figure **3**, an applications page icon **406** for selecting application in accordance with operation **312** of Figure **3**, an event log icon **408** for displaying a log of events in accordance with operation **318** of Figure **3**, and IP address page icons **410** for selecting trusted and untrusted IP address, in accordance with operations **314-316** of Figure **3** Upon selection of the summary page icon **404** in the menu **402**, the summary page **400** is simultaneously displayed in conjunction with the menu **402**.

As shown, the summary page **400** is displayed including a recent activity list **420**, frequently accessed port list **422**, commonly blocked IP address list **424**, and commonly blocked application list **426**. As shown in Figure **4**, the recent activity list **420** includes recent activity icons corresponding to various events.

For example, one icon is reserved to indicate a total number of events within a predetermined time period, while another icon is reserved to represent the recent blocked attempts of the remote computers to access predetermined ports associated with the local computer. Further, additional icons are reserved for representing the recent blocked attempts of the remote computers with the predetermined set of banned IP addresses to access the local computer.

The recent activity list **420** further includes a total number **432** of the events within a predetermined time period corresponding with each recent activity icon, and a graphical representation **434** indicating a severity of the total number of the events.

As mentioned earlier, the graphical representation **434** may include a bar graph for providing a quick reference as to the severity of the tally of each of the

events. For example, a number of dots or other type of character may be used which is proportional to the severity of the total number of events.

The frequently accessed port list **422** includes port icons corresponding to frequently accessed ports, and/or banned ports on which the blocked attempts of the remote computers occurred. The frequently accessed port list **422** further includes a total number of the attempts corresponding with each port icon, and a graphical representation indicating a severity of the total number of the attempts, similar to the previous list.

Still yet, the commonly blocked IP address list **424** includes IP address icons corresponding to banned IP addresses from which the blocked attempts of the remote computers occurred. The commonly blocked IP address list **424** further includes a total number of the blocked attempts corresponding with each IP address icon, and a graphical representation indicating a severity of the total number of the blocked attempts.

In a similar manner, the commonly blocked application list **426** includes application icons corresponding to banned applications associated with the blocked attempts. The commonly blocked application list **426** further includes a total number of the blocked attempts corresponding with each application icon, and a graphical representation indicating a severity of the total number of the blocked attempts.

Figure **5** illustrates an exemplary event log **500** illustrating various traffic events that may be monitored by the firewall, in accordance with operation **318** of Figure **3**. As shown, various categories **502** of traffic events are shown. For example, a "Today" category, a "This Week" category, as well as a "Total" category may be provided. Further, various information may be displayed regarding each event, such as the time and date **504** when the traffic event was logged, the

associated Internet Protocol (IP) address **506**, and other related event information **508**. During use, any of the listed events in the event log **500** may be selected.

Additional features may also be provided. For example, the various lists of traffic events under each category **502** may be collapsed and expanded as desired by selecting icons **510**. By this feature, a user may focus on a category of interest. As a further option, the event log **500** may be archived upon the selection of an archive icon **512**. Still yet, an archived event log **500** may be accessed via a view archived log icon **514**. The present event log **500** may even be cleared using a clear event log icon **518**.

Upon the selection of any of the traffic events in the event log **500**, a lower portion **520** of the event log **500** may be reserved for additional information relating to the selected event. Such information may include, but is not limited to applications associated with the selected event.

As an option, the menu **550** may be simultaneously displayed in conjunction with the event log **500** for providing the user quick and efficient access to other optional features such as a summary page, a list of trusted and banned IP addresses, etc.

Still another portion **522** of the event log **500** may include a plurality of tools for processing a selected traffic event. For example, a report icon **524** may be selected in order to transmit intrusion activity information to a central server for analysis. Other features may include an option to record the selected event, identify additional information on the selected event, allow traffic on a port associated with the selected event, allow the receipt of traffic from an IP address associated with the selected event, and disallow the receipt of traffic from an IP address associated with the selected event. Of course, any desired functionality may be incorporated per the desires of the user.

As an option, various color coding schemes may be used in the conjunction with the present embodiment. For example, entries of a first color may indicate events from a local IP or non-routable IP (e.g. 192.168.X.X). Further, entries of a second color may be from a possibly spoofed IP address, such as the loopback adapter (127.0.0.1) or an invalid IP (0.0.0.0). Still yet, entries of a third color (i.e. red) may be from banned IP addresses.

Figures **6A-6F** illustrate a plurality of options available to the user of the firewall, in accordance with various embodiments.

Figure **6A** illustrates a security feature **600** that allows a user to utilize a slider bar **602** for setting a traffic blocking level. The traffic blocking level may be set by sliding the slider bar **602** to the desired blocking level. The blocking level ranges from completely open (Low) to completely closed (High). Table #1 elaborates on such levels.

Table #1

Setting	Description
Open	Firewall is effectively disabled. All traffic is allowed through with no filtering.
Trusting	Any computer with which one initiates a connection will be trusted for IP traffic on the same port, and UDP on any port. This setting should be chosen when the user finds that some games or streaming media will not work.
Standard	(Recommended) Only computers with which the user initiates communications will be allowed to send traffic back.

Tight	Only traffic that consists of direct replies to requests from a computer will be allowed. On this setting many applications which use UDP packets (mostly games and programs that 'stream' video or audio) will not be able to get traffic.
Lock-Down	All traffic is stopped. This is essentially the same as unplugging an Internet connection. Even ports that have been configured to be open using the applications options will be blocked.

HOME\5085.0202

As shown in Figure **6A**, various options **604** may be employed by the user. One may choose whether or not to log any events that the personal firewall reports. Immediate background traces may also be enabled to perform a trace on an event and log it in the event log for future reference. Still yet, one may choose to accept ICMP ping requests. In other words, one may set the behavior of blocking and logging for ICMP traffic. ICMP traffic is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If the user is utilizing or has utilized a peer to peer file sharing program, he or she may find themselves being pinged a lot.

Table #2 illustrates the various options associated with the ICMP traffic

Table #2

- **No-Log/Alert me** blocks the ping request and logs it as an event.
- **No-Ignore** blocks the ping request, but it does not log it.
- **Yes** allows all ping requests without logging them.

Figure **6B** illustrates various additional general options **620** that may also be provided, in accordance with one embodiment. For example, for when an event is detected, a drop-down menu **622** may let the user choose how the personal firewall notifies the user when it detects an event. Table #3 illustrates some options with respect to notifications.

Table #3

- **Flash the Tray Icon:** Select this option to have the personal firewall flash the system tray/notification area icon.
- **Display a warning dialog:** Displays a dialog box and flashes the system tray/notification area icon when the personal firewall detects an event.
- **Keep Quiet:** The personal firewall logs events as it detects them, but it does not display any alerts.

A user may also utilize a variety of check boxes **624** for selecting further options. For example, a user may select to show port numbers in the event log. This displays the source and destination ports of an event. Further, a user may select to show an alert icon in a system tray while the personal firewall is running. Optionally, a user may select to hide an alert dialog box five seconds after it alerts the user about an event.

Various tracing options are also available. For example, a drop down menu may be provided to allow one to select which available visual trace version to use for tracing events. By default, the built-in tracing feature may be selected. As an option, sound effects may be used during the trace. Further, trace caches may be selectively cleared.

Still yet provided in the interface of Figure **6B** is an option to sign up for a hacker-watch service. In order to report events to a hacker-watch service (i.e.

Express Mail No. EV339950742US

HackerWatch.org), one may sign up for the service. Signing up allows submissions to be tracked and allows the service to provide a notification if a hacker-watch server needs more information or further action from the user. The sign up process may also be important to confirm any information received. All email addresses provided to the service may be kept confidential. If a request for additional information is made by an ISP, that request is routed through the hacker-watch service without the user email address being exposed.

Figure **6C** illustrates an option interface **630** associated with designating banned IP addresses, in accordance with one embodiment. As shown, a banned IP address list **632** provides one with a convenient mechanism to completely block traffic from a specific computer. Effectively, the user will be invisible to a computer at that IP address regardless of other settings, and the IP address is banned. In use, if a personal firewall detects an event from a banned IP address, it will alert the user via whichever method is selected in the "When an event is detected drop-down" menu set forth earlier.

Figure **6D** illustrates an option interface **640** associated with designating trusted IP addresses, in accordance with one embodiment. The present option **640** allows a user to enter the IP addresses that they want the personal firewall to trust at all times. If a user is using a computer on an office LAN, and has no reason to block traffic from other computers on that LAN, he or she can instruct the personal firewall to trust all computers on the LAN. This can be accomplished by selecting the check box **642** indicating that all computers on a LAN are trusted. If a LAN is not detected, this option may not be available. Similar to the interface of Figure **6C**, the present interface has Add and Remove icons **644** for facilitating the foregoing process.

In use, the personal firewall trusts any IP addresses in the present list, and always allows traffic from those IPs through the firewall on any port. The personal

10071586.020802

firewall does not necessarily log any events from trusted IP addresses. To computers at a trusted IP, it may be as though no firewall is present.

Figure **6E** illustrates an interface **650** associated with designating trusted applications, in accordance with one embodiment. Some applications need to accept unsolicited connections from other computers to work. In general, these are server programs, such as a web site host or file sharing. For example, a computer does not need to open any ports in order to receive email, but if the computer protected by the personal firewall acts as an email server, then the user may need to open the appropriate ports by checking the appropriate application items. See check boxes **652**.

A user is recommended not to set applications until he or she is certain the ports must be open. A number of common applications and servers that one might be running may be pre-configured for convenience purposes. If one needs to add ports that are not already configured, he or she can add them easily through the options dialog or by simply clicking an event in the event log and creating a rule based on that event.

While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.